Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 35 (2014) 812 – 821

Procedia Computer Science

18th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems - KES2014

Extended abstract digital forensics model with preservation and protection as umbrella principles

Shahzad Saleem[a]*, Oliver Popov[a], Ibrahim Bagilli[b]

[a]*Department of Computer and Systems Sciences, Stockholm University, Forum 100, Isafjordsgatan 39 SE- 16440 Kista, Sweden*

[b]*Department of Computer & Electrical Engineering and Computer Science, University of New Haven, 300 Boston Post Road West Haven, CT 06516, USA*

Abstract

In this research, a literature review was conducted where twenty (n=20) frameworks and models highlighting preservation of the integrity of digital evidence and protection of basic human rights during digital forensic investigations were studied. The models not discussing the process at an abstract level were excluded. Therefore, thirteen (n=13) of the studied models were included in our analysis. The results indicated that published abstract models lack preserving the integrity of digital evidence and protecting the basic human rights as explicit overarching umbrella principles. To overcome this problem, we proposed an extension to Reith's abstract digital forensics model explicating preservation of integrity and protection of human rights as the two necessary umbrella principles.

Peer-review under responsibility of KES International.

Keywords: Digital Evidence, Digital Forensics, Digital Forensics Process Models, Preserving the Integrity of Digital Evidence, Protecting the Basic Human Rights, Abstract digital forensic models, Abstraction

1. Introduction

Digital devices have become an integral part of our lives. Their use is profound and their ability to record our activities with extreme detail transforms them into digital behavioral archives of their respective users[1–4]. Between eighty to ninety percent cases in US involve some form of digital evidence (DE)[5–7]. Digital Forensic Science (DFS) evolved to handle this special kind of evidence. In DFS research is being conducted on technical

* Corresponding author. Tel.: +46 707 713439

E-mail address: shahzads@dsv.su.se

Peer-review under responsibility of KES International.

doi:10.1016/j.procs.2014.08.246

and theoretical fronts[8]. The technical research covers the development of tools to aid in systematic Digital Forensics (DF) investigations. Theoretical research covers the development of theories and methodologies including processes, frameworks and models to conduct DF investigations[8].

This research work is within the domain of theoretical research, which is important because it provides the foundation of DF as a scientific discipline. In addition it stipulates a philosophical account and common understanding for DFS as a scientific discipline[9]. It also assists in (i) the development of abstractions, principles, standards and models which are flexible, technology neutral, and generally acceptable[10,11] (ii) the development of DF process models which are mutually understood, observed and valid in both legal and technical contexts[12] and (iii) embedding scientific rigor, trust and reliability to facilitate education, application and research in DFS[13,14].

A literature review was conducted with twenty (n=20) frameworks and models which are used to conduct DF investigations. Thirteen (n=13) of them were abstract, and were used in our analysis. The results indicated that the models lack preserving the integrity of DE and protecting the basic human rights as *explicit* overarching umbrella principles. To overcome this problem, we proposed an extended abstract DF model explicating the preservation and protection as two necessary umbrella principles (explained in Section 4).

A model is defined as *"the mental image of the world around you"*[15]. It comprises selected *concepts* and their associated *relationships* in the real world system[15]. In the light of the definition of a model, and the results from our literature review, the analyzed abstract DF models have one of the following two inadequacies:

1. They do not consider the activities of preserving the integrity of DE and protecting human rights *(the concept is ignored)* and/or
2. They do not capture and represent their relationship explicitly with other parts of the model which is synonymous to the application of the model in the real world *(the relationship is ignored)*.

To solve these problems, an extension to Reith's abstract DF model[8] was proposed where preservation and protection were included as two explicit overarching umbrella principles. We termed the model as an "extended abstract digital forensics model with 2PasU" where 2PasU stands for *Preservation and Protection as two explicit Umbrella principles*.

The remaining sections of this paper discuss the literature review and its summary, explanation of the concepts of preservation and protection (2PasU), and how they are incorporated into our model. The last section concludes the discussion and indicates about the direction of future research in this domain.

2. Methodology

DF models are a set of processes providing a concise, concurrent, abstract and mutually understandable foundations on which technical development can progress[16]. The literature review of twenty (n=20) models was conducted with an emphasis on abstraction, preservation and protection (as explained below).

1. *Abstract model:* is technology neutral, generic and applicable to every kind of digital crime[8].
2. *Preservation:* Landwehr defines integrity as a phenomenon of "assuring that digital information is not modified (either intentionally or accidentally) without proper authorization"[17]. In DF preserving the integrity of DE as an umbrella principle is important because (i) one of the most quoted DF models "Investigative process of digital forensics science"[18] highlights the importance of preservation as an umbrella principle. It includes the notion of preservation as one of the seven classes and also as a method to all the four classes considered "forensic" (ii) DE in its nature is messy, massive, slippery, abstract and transformed interpretation of reality[19,20] and (iii) holding the integrity and thus the fidelity of DE is not easy because of its nature. This fact can consequently shatter the confidence in the veracity of DE upon which decision-makers act[18].
3. *Protection:* DF is applied in the areas of (i) Law Enforcement (ii) Military Information Warfare Operations and (iii) Business & Industry[18]. During the review, frameworks and models were studied from the

investigative context of law enforcement settings[10]. The goal in law enforcement settings is to produce reliable and admissible evidence under an ordered list of constraints comprising Law, Time, Resources and Technical Limits (in order of preference)[10]. Therefore, compliance to the law is the most important constraint. Law with its tools strives to maintain a balance in a society and one of its cornerstones is the protection of the human rights. Edward Snowden's revelations are just an example of possible human rights violations in our digital world[21]. So, protection of human rights must be given foremost importance because it is central to the contemporary civilized society and the discipline of DF.

Following inclusion and exclusion criteria were used during the process of review:

1. *Inclusion criteria:* The models and frameworks describing the process of DF with preservation and protection attributes were included in this review.
2. *Exclusion criteria:* The models and frameworks not describing the process of DF at an abstract level were excluded. So, the models describing the technical details and those providing a realization of an abstract DF model were excluded.

3. Literature review

Seven out of the twenty frameworks and models discussing preservation and protection were not on abstract level and hence excluded from our analysis. The remaining thirteen frameworks and models were analyzed, qualified and tagged with "Yes", "To Some Extent (TSE)" or "No" for preservation and protection using the following criteria.

- *Preservation:* If a model discussed preservation during the entire forensics process in the form of an explicit notion of chain of custody, documentation, reproducibility and or non-interference then the model was tagged with a "Yes" for preservation as an umbrella principle. Although we tagged some models with a "Yes" for preservation but it was observed that most of them failed to capture the concept and its full relationship with the rest of the model in the graphical representation. We improved our solution by discussing the concept and the relationship along with capturing the representation of the both in the graphical form. If a model discussed preservation just prior to collection, partial documentation of evidence and or an implicit notion of chain of custody then the model was tagged with "TSE". If a model did not discuss preservation at all then it was tagged with a "No".
- *Protection:* If a model discussed protection during the entire length of a forensics process and also captured it in the graphical representation then the model was tagged with a "Yes" for protection. These models stressed the need of authorization, minimization, bringing the litigating parties closer to the investigative process, guaranteeing the preservation, privacy and or fulfillment of legal requirements for the entire length of the forensics process. The model was tagged with "TSE" if the above concepts were discussed for some parts of it and with a "No" if the concepts were neither discussed nor captured in the graphical representation.

3.1. Results of the literature review

Table 1 is the summary of the results from the review process. Please note that Ieong 2006[22] is a role-based framework so it cannot be used in comparative analysis with the rest of the activity based frameworks and models. Therefore, it was excluded from the discussion in the results sub-section. First column in Table 1 shows all the models which were studied and the one at the end is proposed in this article. Second column describes whether the model/framework was at the abstract level or not. Third column tells about the level of preservation as an umbrella principle, and the last column shows the level of protection as an umbrella principle.

From Table 1, it is evident that preservation is discussed by many of the frameworks and models but only

some of them have really captured its relationship with the other sub-processes by considering it as an umbrella principle. Some models considered protection of human rights in the form of privacy and conformance to the local law, rules and regulation. But almost all of them do not consider protection as an umbrella principle. In all the models, the subjects have to trust the process as a black box. Intentional and or unintentional modifications, for instance by an unethical insider, can adversely affect many basic human rights. Therefore, we noted that 2PasU must be explicitly identified and captured during the definition of an abstract model. The section below will describe in detail the concept of 2PasU, which is incorporated in our proposed extended abstract model.

Table 1: Summary of the review

Model/Framework	Abstract	Preservation	Protection
Reith 2002[8]	Yes	TSE	No
Pollitt 2007[9]	No		
Mocas 2004[10]	Yes	Yes	TSE
Carrier 2004[11]	Yes	Yes	TSE
Pollitt 1995[12]	Yes	No	TSE
Beebe 2005[13]	Yes	Yes	No
Ruibin 2005[14]	No		
Pollitt 2004[16]	No		
Palmer 2001[18]	Yes	Yes	No
Ieong 2006[22]	Yes	Yes	Yes
Noblett 2000[23]	Yes	Yes	No
NIJ 2001[24]	Yes	TSE	TSE
Carrier 2003[25]	Yes	Yes	TSE
Agarwal 2011[26]	Yes	Yes	TSE
Baryamureeba 2004[27]	Yes	TSE	TSE
Shin 2011[28]	Yes	TSE	No
Carrier 2003[29]	No		
Kent 2006[30]	No		
Ma 2011[31]	No		
Stephenson 2003[32]	No		
Model with 2PasU	Yes	Yes	Yes

4. Preservation and protection (2PasU)

This section is devoted to the description of preservation of the integrity of DE and protection of the basic human rights during the process of DF as umbrella principles. It will also explain the term basic human rights in the context of DF.

Evidence is the backbone of our judicial system. DE is an evolved form of traditional evidence, inheriting most of the complexities of the latter, while adding more of its own. It is a well-known fact that evidence can and has been manufactured, planted, and or taken out of the context to wrongly convict or acquit people[33].

Most people tend to be more careful of what they commit on paper or over a phone, however they may not act in the same way when using digital systems such as e-mails, blogs and online discussion forums[33] from where evidence can be obtained. Furthermore, evidence is usually more compelling than the eye witness's

testimony[33]. Therefore, preserving the integrity of DE and protecting basic human rights as explicit umbrella principles is critical during a forensic investigation.

4.1. Preserving the integrity of digital evidence as an umbrella activity

DE is rich, abstract and volatile[19,20]. To explain the volatility, consider a captured dump of a network. It is actually a snapshot of the system at a particular instance of time t_1 and the original will not be the same at any other time t_2. So, at t_2, there will exist nothing to compare the image taken at t_1 and hence verify its integrity. Similar is the case with mobile device forensic images and other live systems. Hence, it is essential to seal the master image in such a way that problems arising due to the volatility of the DE are mitigated. Therefore setting the theoretical foundation of preserving the integrity of DE as an umbrella principle is an important aspect which must be explicitly outlined in the abstract DF model.

4.2. Protecting the basic human rights as an umbrella activity

The proposed model stands at abstract level. So, what we present in this section is not an exhaustive list of the human rights at stake during the DF process. Privacy (soft and hard), right to know and right of a fair trial are the important ones discussed in the section below.

Privacy is defined as the *"right to be let alone, and the right to the informational self-determination"*[34]. It enables people to *"control, edit, manage, and delete information about themselves and decide when, how and to what extent that information is communicated to others"*[34]. The concept of privacy is broad, difficult to define and circumscribe[35]. The Fourth amendment of the constitution of the United States protects the people from unreasonable search and seizure[36]. Many countries either explicitly place the right to privacy in their constitution or their courts have recognized this right through other provisions[37].

The literature illustrates many specialized solutions to protect the privacy of the parties involved in the DF process. Reddy and Venter[38] presented a framework to achieve forensic readiness for privacy incidents. Law et al.[39] proposed a cryptographic model to protect the privacy during any forensic investigation. To balance the requirements of both privacy and forensics, Croft and Olivier[40] suggested the sequential release of privacy-accurate information in a forensic investigation. Their layered system decouples the identity from the data to the point where that association is really required. Therefore, it reveals the identity of only the relevant entities.

Antoniou et al.[41] proposed a forensics investigation protocol *"Protect Private Information, Not Abuser"*. This protocol allows the user to surf the Internet anonymously unless the server has gathered enough evidence that the user is a potential attacker. In this case, the forensic investigation entity comes into play and reveals the identity of the attacker after the necessary investigation. Bohannon et al.[42] described a framework based on cryptography to handle the privacy issues in forensic DNA databases. Hou et al.[43] discussed the privacy concerns associated with shared remote servers. They also presented a cryptographic solution based on homomorphic and commutative encryption.

Preserving the integrity of DE and protecting privacy are important concerns for forensic investigations in cloud computing infrastructure[44]. Problems of jurisdiction, lack of international collaboration, legislative mechanism in cross-nation data access/exchange, lack of law/regulation and law advisory are some of the most important challenges identified by Keyun et al. in the context of clouds[45].

Digital investigations are restricted by national and international legislation which is more restrictive in case of civil litigation. Police and Criminal Evidence Act 1984[46], Computer Misuse Act 1990[47], Electronic Communications Privacy Act of 1986[48], Article 5 of the European Convention on Human Rights[49], Regulation of Investigatory Powers Act 2000[50], EU directive for Protection of personal data[51] are only a few examples of these restriction. Usually the constitution, legislation and the related tools place limits on "what" can be processed and not on "how" it can be processed. To this end Adams[52] proposed the development of a forensic

tool with a facility to record all the steps it takes during an investigation.

A brief discussion of soft and hard privacy concepts in the context of forensic investigation can help to place limits on "how" the data is processed. The idea behind the hard privacy is to reduce the need to trust other parties and to share as little data as possible. In soft privacy, the subjects lose the control over their personal data and have to trust the competence and the honesty of those who control the data.[34]

In the context of a forensic investigation the subjects also lose their control over their personal data, out of which only a small portion might be relevant to the case. The entire process of a digital forensic investigation is like a black box to most of the subjects. Subjects have to trust the correctness of the overall process, the competence and integrity of the individual involved in carrying out the process. Concepts from the field of security are equally applicable to DFS. From the study of security we know that insiders are the greatest threat[53] and human beings are the weakest link[54] to the overall security of a system. Therefore, subjects should be given the "right to know" about not only "what" but also "how" the data is being processed to protect their soft privacy.

The analogy of the "Right to Know" from community and environmental law of the United States has been fetched into the domain of DF investigation. It can also help in upholding the "Right of a Fair Trial" which must ensure that no one should be wrongly convicted or acquitted either intentionally or unintentionally. If Forensic investigation is not conducted properly then it can affect many basic human rights[55] as a consequence of a wrong conclusion or decision. "The Amero case: Mousetrapping and Pagejacking" and The "Garlasco" case: the "IT alibi"[56] are the two examples in this context.

Investigating organizations must regularly define, update and enforce competence requirement and conduct proficiency testing[57]. This can raise the level of quality assurance, soundness of the forensics investigation and consequently help in protecting the basic human rights.

The constitution, legislation and the related tools to safeguard the basic human rights and various research contributions to balance the requirements of privacy and forensics by specialized solutions encouraged us to explicitly include 2PasU in the extended abstract model. The model will not only highlight the importance of 2PasU but will also inspire the development of more specialized solutions in this context. Such an extended model with 2PasU is discussed in Section 5.

5. Extended abstract digital forensics process model with 2PasU

A literature review of the frameworks and models to perform DF at an abstract level revealed the absence of 2PasU. An extension to the Reith's abstract models was proposed to overcome the problem. The extension is inspired from the research related to preservation and protection (Section 4). The model fulfills functional requirements of forensic investigations with the help of seven sub-processes and non-function qualitative requirements with two overarching explicit umbrella principles. These principles include preserving the integrity of DE and protecting the basic human rights during the entire course of the forensic process.

5.1. Overarching principles

Preservation and Protection as defined and described in Section 4 are the two overarching principles colored grey in Figure 1. Since it is an abstract model and we are discussing the principles so the list of activities to fulfill these principles is flexible including but not limited to the important ones discussed below.

1. *Preservation:* Activities included in preservation are (i) preserving the integrity of DE and the platform used for investigation, (ii) documentation and the chain of custody encompassing the overall process and (iii) isolating and preserving the containers of DE.
2. *Protection:* is about protecting the basic human rights including but not limited to (i) privacy both hard and soft (ii) right to know and (iii) right of a fair trial. Some risks in this context can be mitigated if the subjects

are brought closer to the ongoing digital forensic investigation in such a way that the process no longer remains a black box to them.

5.2. The model with 2PasU

Our proposed model is inspired from Reith's work[8]. It consists of the following list of ordered sub-phases: *(1) preparation and planning (2) collection (3) examination (4) analysis (5) reporting (6) presentation, (7) archiving and returning evidence.* Sub-Phases namely collection, examination, analysis and reporting are the core forensic activities (colored green in Figure 1) while the rest of them are significant forensic activities (colored blue in Figure 1). Explanation to these phases is given below:

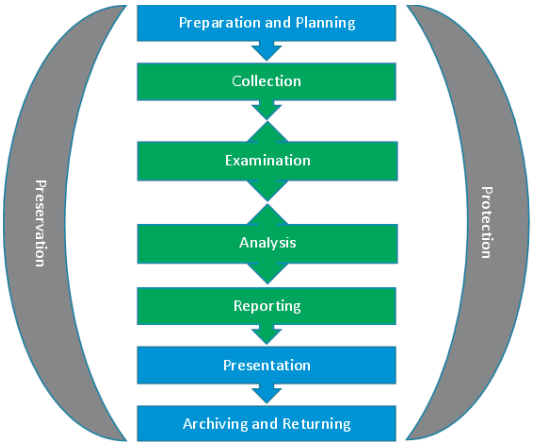

Fig. 1. Extended Abstract Digital Forensic Model with 2PasU

1. *Preparation and planning:* Activities in this sub-process are not considered real forensics. However, this sub-process is the starting point of the investigation. Decisions made during this stage will affect all the subsequent sub-phases. Therefore, taking informed decisions at this stage is crucial.
   The basic goal of a forensic investigation is to help provide justice and to protect the basic human rights of all the involved entities. Before the raid, an investigator should gather knowledge about the incident to decide its type and the requirements. It will enable the investigator to prepare and plan in the light of guidelines, best practices, principles, policies, and relevant legislation, to fulfill the requirement of 2PasU. The preparation will help gather the most relevant evidence by spending the least amount of resources[58]. The preparation will assist to select the right tool[1,3,59,60], to fulfill the necessary legal requirements (warrants and authorizations), to decide the level of management (documentation and chain of custody), and to arrange necessary support (reinforcements).
   Since the model is abstract as well as flexible, so investigators decide the level of importance to be given to 2PasU during this phase following the requirements of the case. We anticipate that 2PasU plays a more important role in civilian law enforcement when compared to military settings.
2. *Collection:* Deals with preserving the physical evidence and collecting the DE in the form of replicas following the requirements of 2PasU. Working on the replicas is the norm in DF, so subjects should also be given these replicas with an aim to bring them closer to the ongoing investigation. By doing so they will not

have to trust the process as a black box. Depending on the consequences, subjects can also privately run the investigation on these replicas to confirm the conclusions drawn by other experts (*right of a fair trial*).

3. *Examination:* of the replica to identify potentially relevant DE in the light of preparation and planning phase. Although the order of the steps is preserved in this model but if the requirements of 2PasU are relaxed for instance, in military settings then both collection and examination phases can be fused together to perform DF triage with an aim to quickly reach to the conclusions[58].
4. *Analysis:* is concerned with building and supporting a crime theory with the help of relevant and weighty DE. The process from collection to analysis can be iterated many times before reaching to the correct conclusions while fulfilling the requirements of 2PasU.
5. *Reporting:* constitute an expert's conclusions along with the relevant and weighty DE. It deals with summarizing the findings, providing the explanations and conclusions along with the appropriate DE. It is written for a layman using abstract terminologies with suitable references and the evidence following 2PasU. For instance, 2PasU in this sub-phase will require that the reports must have associated chain of custody and signed hashes.
6. *Presentation:* is an art to infer from DE using logic and common sense. The output of the reporting sub-phase becomes an input for presentation. The aim of this phase is to present the findings in such a way that relevance and weight of the DE is established to the case at hand. In the mind of the trier of the fact, it will create an argument for the existence or non-existence of some other matter of fact thus helping in solving or furthering a specific case. Any questions related to 2PasU are also answered during this phase.
7. *Archiving and returning:* deals with strictly securing and sealing the DE along with all the output of 2PasU for any potential future usage. All the forms of evidence seized during the investigation are returned to their owners. Any necessary deletion, purging and destruction to protect the basic human rights is also executed during this phase.

6. Conclusions and future work

Instead of discrete steps in the model, preservation and protection are taken out in the form of umbrella principles. The model in Figure 1 now depicts all the important concepts and their relationships with each other and thus conforming to the definition of a mental model as well. The model gives due importance to both preservation and protection as overarching principles. Hence any future specialized development or realization of this model will automatically emphasize on both of these qualitative aspects. In the same time, 2PasU are abstract and thus can include a flexible list of activities for each abstract sub-process depending on the requirements and the contextual operational settings.

In the future, we will present a realization of this abstract model in the form of a technical solution operable on the collection sub-phase. Requirements of 2PasU will be fulfilled by employing the latest tools and technology in the form of add-on solutions that can extend the capabilities of existing DF tools.

References

1. Saleem S, Popov O. Formal Approach for the Selection of a Right Tool for Mobile Device Forensics. *5th International Conference on Digital Forensics & Cyber Crime*. Moscow; 2013.
2. Casey E. *Digital evidence and computer crime: forensic science, computers, and the Internet*. 3rd ed. 2011.
3. Saleem S, Popov O, Kubi A. Evaluating and Comparing Tools for Mobile Device Forensics using Quantitative Analysis. Rogers M, Seigfried-Spellar KC, editors. *Digit Forensics Cyber Crime Lect Notes Inst Comput Sci Soc Informatics Telecommun Eng*. Lafayette: Springer Berlin Heidelberg; 2013;114:264–82.
4. International Telecommunication Union (ITU). *ICT Facts and Figures* [Internet]. 2013 [cited 2013 Sep 23]. Available from: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf

5. Rogers MK. DCSA: *A Practical Approach to Digital Crime Scene Analysis* [Internet]. West Lafayette: Department of Computer Technology, Purdue University; 2004 [cited 2013 Jan 17]. Available from: http://www2.tech.purdue.edu/cit/Courses/cit556/readings/DCSA.pdf
6. Baggili I, Mislan R, Rogers M. Mobile Phone Forensics Tool Testing: A Database Driven Approach. *Int J Digit Evidence.* 2007;6(2).
7. Science Daily. *Digital Evidence Cyber Forensic Researchers Make The Call: Crime Scene Evidence Is Quickly Extracted From Mobile Phones* [Internet]. 2009 [cited 2013 Jun 26]. Available from: http://www.sciencedaily.com/videos/2009/0104-digital_evidence.htm
8. Reith M, Carr C, Gunsch G. An Examination of Digital Forensic Models. *Int J Digit Evid*. 2002;1(3):1–12.
9. Pollitt M. An ad hoc review of digital forensic models. *Syst Approaches to Digit Forensic*. 2007;43–54.
10. Mocas S. Building theoretical underpinnings for digital forensics research. *Digit Investig*. 2004 Feb;1(1):61–8.
11. Carrier B. An event-based digital forensic investigation framework. *Proceedings of Digital Forensic Research Workshop*. 2004.
12. Pollitt M. Computer Forensics: an Approach to Evidence in Cyberspace. *Proceedings of the National Information Systems Security Conference*. 1995. p. 487–91.
13. Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. *Digit Investig*. 2005 Jun;2(2):147–67.
14. Ruibin G, Yun T. Case-relevance information investigation: binding computer intelligence to the current computer forensic framework. *Int J Digit.* 2005;4(1):1–13.
15. Forrester J. Counterintuitive behavior of social systems. *Theory Decis*. 1971;2:109–40.
16. Pollitt M. Six Blind Men from Indostan. *Digit Forensic Res Work*. 2004;
17. Landwehr CE. Computer security. *Int J Inf Secur*. 2001;1(1):3–13.
18. Palmer G. A Road Map for Digital Forensic Research. *Digit Forensic Res Work*. Utica, New York; 2001;
19. Casey E. Challenging Aspects of Digital Evidence. *Digital evidence and computer crime: forensic science, computers, and the Internet.* 3rd ed. 2011. p. 25–8.
20. Farmer D, Venema W. Forensic Computer Analysis: An Introduction. *Dr Dobbs J*. M and T Publishing Inc.; 2000;25(9):70–5.
21. Greenwald G, Scahill J, Poitras L. *The Intercept* [Internet]. [cited 2014 Feb 12]. Available from: https://firstlook.org/theintercept
22. Ieong RSC. FORZA – Digital forensics investigation framework that incorporate legal issues. *Digit Investig*. 2006 Sep;3:29–36.
23. Noblett MG, Pollitt MM, Presley LA. Recovering and examining computer forensic evidence. *Forensic Sci Commun*. 2000;2(4):102–9.
24. National Institute of Justice. *Electronic crime scene investigation: A guide for first responders* [Internet]. 2001 [cited 2012 Feb 15]. Available from: https://www.ncjrs.gov/txtfiles1/nij/187736.txt
25. Carrier B. Getting physical with the digital investigation process. *Int J Digit Evid*. 2003;2(2):1–20.
26. Agarwal A, Gupta M, Gupta S, Chandra S. Systematic Digital Forensic Investigation Model. *Int J Comput Sci Secur*. 2011;5(1):118–31.
27. Baryamureeba V, Tushabe F. The enhanced digital investigation process model. *Proceedings of the 4th Annual Digital Forensic Research Workshop*. 2004. p. 1–9.
28. Shin Y-D. New Model for Cyber Crime Investigation Procedure. *J Next Gener Inf Technol*. 2011 May 31;2(2):1–7.
29. Carrier B. Defining digital forensic examination and analysis tools using abstraction layers. *Int J Digit Evid*. 2003;1(4):1–12.
30. Kent K, Chevalier S, Grance T, Dang H. *Guide to integrating forensic techniques into incident response* [Internet]. NIST SP800-86 Notes. 2006 [cited 2012 Mar 13]. Available from: http://cybersd.com/sec2/800-86Summary.pdf
31. Ma G, Sun C, Wang Z. Study on digital forensics model based on data fusion. *Int Conf Mechatron Sci Electron Eng Comput.* 2011;898–901.
32. Stephenson P. Modeling of post-incident root cause analysis. *Int J Digit Evid*. 2003;2(2):1–16.
33. Caloyannides M. *Privacy Protection and Computer Forensics*. Second. Artech House; 2004.
34. Deng M, Wuyts K, Scandariato R, Preneel B, Joosen W. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requir Eng*. 2010 Nov 16;16(1):3–32.
35. Michael J. *Privacy and human rights: an international and comparative study, with special reference to developments in information technology*. Dartmouth Pub. Co.; 1994.
36. Aminnezhad A, Dehghantanha A, Abdullah MT. A Survey on Privacy Issues in Digital Forensics. *Int J Cyber-Security Digit Forensics*. 2012;1(4):311–23.
37. Global Internet Liberty Campaign. *Privacy and human rights: an international survey of privacy laws and practice* [Internet]. 1999 [cited 2014 May 6]. p. 1–16. Available from: http://gilc.org/privacy/survey/intro.html
38. Reddy K, Venter H. A Forensic Framework for Handling Information Privacy Incidents. *Adv Digit Forensics V*. 2009;143–55.
39. Law FYW, Chan PPF, Yiu SM, Chow KP, Kwan MYK, Tse HKS, et al. Protecting Digital Data Privacy in Computer Forensic Examination. *Sixth IEEE Int Work Syst Approaches to Digit Forensic Eng*. IEEE; 2011 May;1–6.
40. Croft NJ, Olivier MS. Sequenced release of privacy-accurate information in a forensic investigation. *Digit Investig*. Elsevier Ltd; 2010 Oct;7(1-2):95–101.
41. Antoniou G, Wilson C, Geneiatakis D. PPINA–a forensic investigation protocol for privacy enhancing technologies. *Commun Multimed Secur*. 2006;1–11.

42. Bohannon P, Jakobsson M, Srikwan S. Cryptographic approaches to privacy in forensic DNA databases. *Public Key Cryptogr*. 2000;
43. Hou S, Uehara T, Yiu SM, Hui LCK, Chow KP. Privacy Preserving Confidential Forensic Investigation for Shared or Remote Servers. *Seventh Int Conf Intell Inf Hiding Multimed Signal Process*. IEEE; 2011 Oct;378–83.
44. Damshenas M, Dehghantanha A, Mahmoud R, bin Shamsuddin S. Forensics investigation challenges in cloud computing environments. *International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*. IEEE; 2012. p. 190–4.
45. Ruan K, Carthy J, Kechadi T, Baggili I. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digit Investig*. Elsevier Ltd; 2013 Jun;10(1):34–43.
46. Home Office of the Great Britain. *Police and Criminal Evidence Act (PACE) codes of practice* [Internet]. 1984 [cited 2014 Jan 15]. Available from: https://www.gov.uk/police-and-criminal-evidence-act-1984-pace-codes-of-practice
47. Home Office of the Great Britain. *Computer Misuse Act* [Internet]. 1990 [cited 2014 Jan 15]. Available from: http://www.legislation.gov.uk/ukpga/1990/18/contents
48. US Department of Justice. *Electronic Communications Privacy Act* [Internet]. 1986 [cited 2014 Jan 15]. Available from: http://www.justice.gov/jmd/ls/legislative_histories/pl99-508/cr-h4039-47-1986.pdf
49. European Commission. *Article 5 of the European Convention on Human Rights* [Internet]. 1950 [cited 2014 Jan 15]. Available from: http://www.hrcr.org/docs/Eur_Convention/euroconv3.html
50. Home Office of the Great Britain. *Regulation of Investigatory Powers Act* [Internet]. 2000 [cited 2014 Jan 14]. Available from: http://www.legislation.gov.uk/ukpga/2000/23/contents
51. European Commission. *Protection of personal data* [Internet]. 2012 [cited 2014 Jan 15]. Available from: http://ec.europa.eu/justice/data-protection/
52. Adams CW. Legal Issues Pertaining to the Development of Digital Forensic Tools. *Third International Workshop on Systematic Approaches to Digital Forensic Engineering*. IEEE; 2008. p. 123–32.
53. Perez JC. *Biggest Security Threat? Insiders* [Internet]. 2002 [cited 2012 Apr 4]. Available from: http://www.pcworld.com/article/105528/biggest_security_threat_insiders.html
54. SANS. *The Weakest Link: The Human Factor Lessons Learned from the German WWII Enigma Cryptosystem* [Internet]. SANS Information Security Reading Room. 2001 [cited 2012 Apr 3]. Available from: http://www.sans.org/reading_room/whitepapers/vpns/weakest-link-human-factor-lessons-learned-german-wwii-enigma-cryptosystem_738
55. United Nations. *UN Universal Declaration of Human Rights* [Internet]. 1997 [cited 2014 Jan 14]. p. 1–6. Available from: http://www.hrweb.org/legal/udhr.html
56. Vaciago G. *Digital Forensics , Privacy and Due Process Rights* [Internet]. Macau; 2013 [cited 2014 Jan 13]. Available from: http://www.slideshare.net/TechAndLaw/digital-forensics-privacy-and-due-processrights
57. International Organization on Computer Evidence. *IOCE - Guidelines for Best Practice in the Forensic Examination of Digital Technology*. 2002.
58. Saleem S, Baggili I, Popov O. Quantifying relevance of mobile digital evidence as they relate to case types: A survey and a guide for best practices. *Journal of Digital Forensics, Security and Law* (Submitted). 2014.
59. Kubi A, Saleem S, Popov O. Evaluation of some tools for extracting e-evidence from mobile devices. *Application of Information and Communication Technologies*. Baku: IEEE; 2011. p. 603–8.
60. Saleem S, Popov O, Baggili I. Right of a Fair Trial and Selection of the Right Tool for Mobile Device Forensics. 2014.